

Privacy Policy

Effective Date: [DATE]

Last Updated: [DATE]

Legal Entity: Kaizen Health Technologies Private Limited (operating brand: "KramOS")

Registered Office: [REGISTERED ADDRESS], Bengaluru, Karnataka, India

CIN: [CIN NUMBER]

Privacy contact: privacy@kramos.health

Grievance Officer: [NAME], grievance@kramos.health

1. INTRODUCTION

At KramOS, privacy is not a compliance afterthought — it is a foundation of the work. The Services we build hold some of the most sensitive information a person ever generates: their medical record. We have written this Privacy Policy to be as clear as we can make it about what we collect, why we collect it, how we use it, and what rights you have in relation to it.

This Privacy Policy describes how Kaizen Health Technologies Private Limited ("KramOS," "we," "us," "our") collects, processes, stores, shares, and protects Personal Data in connection with:

- The KramOS website at <https://kramos.health> (the "Site");
- The KramOS suite of products under the "Kaizen" family (collectively, the "Services");
- Waitlist signups, demonstrations, free trials, paid Subscriptions, and any related communications, including over WhatsApp.

This Policy is governed by the **Digital Personal Data Protection Act, 2023** (the "DPDP Act"), the **Information Technology Act, 2000**, the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** (the "SPDI Rules"), and all other applicable Indian laws.

By using the Site or the Services, you confirm that you have read and understood this Privacy Policy.

2. WHO WE ARE

KramOS is the operating brand of **Kaizen Health Technologies Private Limited**, a private limited company incorporated under the Companies Act, 2013, with its registered office in Bengaluru, Karnataka, India.

For Personal Data we collect directly from website visitors, waitlist signups, and individual subscribers, we act as a **Data Fiduciary** under the DPDP Act.

For Patient Data uploaded to or generated within the Services by a hospital, clinic, or treating medical professional, we act as a **Data Processor** on behalf of that Institution or medical professional, who is the Data Fiduciary in respect of such Patient Data.

This distinction is important and is explained further in clauses 4 and 9 below.

3. DEFINITIONS

For the purposes of this Privacy Policy:

- **"Data Principal"** means the individual to whom Personal Data relates, as defined under the DPDP Act.
 - **"Data Fiduciary"** means the entity that determines the purpose and means of processing Personal Data.
 - **"Data Processor"** means an entity that processes Personal Data on behalf of a Data Fiduciary.
 - **"Personal Data"** means any data about an individual who is identifiable by or in relation to such data.
 - **"Sensitive Personal Data or Information"** ("SPDI") has the meaning given under the SPDI Rules and includes financial information, health information, sexual orientation, and biometric information.
 - **"Patient Data"** means data relating to an identified or identifiable patient that is uploaded to, generated by, or processed through the Services by an Institution or treating medical professional.
 - **"Services"** has the meaning given in the KramOS Terms and Conditions.
-

4. WHAT PERSONAL DATA WE COLLECT

We collect Personal Data in several categories, depending on how you interact with KramOS.

4.1 Information you provide directly

- **Account information:** Name, designation (e.g. intern, resident, consultant, professor, HOD, hospital owner), medical registration number, specialty, professional qualifications, email address, mobile number, WhatsApp number, hospital affiliation, and password (stored in hashed form).
- **Waitlist and demo requests:** Name, hospital, role, email, WhatsApp number, and any free-text message you submit.
- **Subscription and billing information:** Billing address, GSTIN (if applicable), invoicing email, and the last four digits of a payment instrument or UPI handle (full card or bank details are handled by payment processors, not stored by us).
- **Communications:** Records of emails, support tickets, WhatsApp messages, and any other correspondence with us.

4.2 Information collected automatically

- **Usage data:** Pages viewed, features used, click events, session duration, in-product actions, error logs.
- **Device and technical data:** IP address, device type, operating system, browser type and version, browser language, time zone, screen resolution.
- **Cookies and similar technologies:** As described in clause 11 below.

4.3 Patient Data (processed on behalf of Institutions)

When the Services are used in a clinical setting, the relevant Institution or medical professional uploads or generates Patient Data, which may include:

- Patient name, age, sex, contact details, address, and identifiers (such as UHID);
- Clinical notes, examination findings, vitals;
- Investigations ordered and results;
- Diagnoses, prescriptions, and treatment notes;
- Imaging and laboratory reports;
- Hospital admission, transfer, and discharge information;
- Procedure and operative notes.

KramOS processes Patient Data **solely on the instructions of the Institution** that is the Data Fiduciary, and only for the purpose of providing the Services. We do not use Patient Data for any other purpose.

4.4 Information we do not collect

- We do not collect government-issued identification documents (such as Aadhaar, PAN, or passport) for the purpose of website use, except where required by law for institutional onboarding or KYC.
 - We do not collect full payment card numbers, CVVs, or net banking credentials.
 - We do not access your device's microphone, camera, or contact list unless you explicitly grant permission for a specific feature.
-

5. HOW WE COLLECT PERSONAL DATA

We collect Personal Data through:

- Direct submission by you (forms, account creation, waitlist signup, subscription, correspondence);
 - Automated collection (cookies, server logs, analytics);
 - Upload by an Institution or treating medical professional (in the case of Patient Data);
 - Communication with us through email, WhatsApp, telephone, or in-person meetings.
-

6. WHY WE PROCESS PERSONAL DATA

We process Personal Data for the following purposes:

6.1 To provide the Services — creating and managing accounts, authenticating users, delivering features, providing technical support, and operating the Services securely and reliably.

6.2 To process payments — billing, invoicing, payment reconciliation, refunds, GST compliance.

6.3 To communicate with you — responding to enquiries, sending Service-related notifications, scheduling demonstrations, processing waitlist signups.

6.4 To send marketing communications — only with your consent, in accordance with clause 18 below.

6.5 To improve the Services — analytics, troubleshooting, debugging, performance monitoring, product research (using aggregated or de-identified data wherever possible).

6.6 To comply with legal obligations — including under the DPDP Act, the IT Act, tax laws, and any lawful request from authorities.

6.7 To enforce our rights — including under the Terms and Conditions and applicable law.

6.8 For research, development, and quality improvement — using **de-identified or aggregated** data only, never using identifiable Patient Data without the Institution's instructions and any necessary patient consent.

7. LEGAL BASIS FOR PROCESSING

Under the DPDP Act, we process Personal Data on one or more of the following legal bases:

- **Consent** — for marketing communications, optional analytics, and where consent is otherwise required by law;
- **Performance of a contract** — to provide the Services you have subscribed to;
- **Legal obligation** — to comply with applicable Indian laws (e.g. tax, audit);
- **Legitimate uses ("certain legitimate uses" under the DPDP Act)** — for purposes such as fraud prevention, network security, and dispute resolution, where permitted.

Where consent is the basis of processing, you may withdraw your consent at any time as described in clause 15.

8. SENSITIVE PERSONAL DATA AND HEALTH INFORMATION

We treat health information, biometric information, and financial information as **Sensitive Personal Data**, regardless of whether it relates to a user of the Services or to a patient whose data is processed within the Services.

For Sensitive Personal Data:

- We collect only what is necessary for the purpose;
 - We apply enhanced security controls (encryption in transit and at rest, role-based access controls, audit trails, restricted administrative access);
 - We do not share such data with third parties except as described in clause 11, and never for advertising or commercial profiling.
-

9. PATIENT DATA — KramOS AS DATA PROCESSOR

This clause sets out our role and responsibilities in respect of Patient Data, which is distinct from our role in respect of website visitors and individual subscribers.

9.1 Roles. The Institution (or, where applicable, the treating medical professional) is the **Data Fiduciary** for Patient Data uploaded to or generated within the Services. KramOS is the **Data Processor**.

9.2 Purposes. KramOS processes Patient Data solely:

- To provide the Services to the Data Fiduciary;
- As instructed by the Data Fiduciary;
- To comply with legal obligations applicable to KramOS as a Data Processor.

9.3 Consents. The Data Fiduciary is responsible for obtaining all consents and providing all notices required under the DPDP Act and other applicable laws before uploading any Patient Data to the Services.

9.4 Prohibited uses. KramOS does not:

- Use Patient Data for KramOS's own purposes;
- Sell, rent, or commercially exploit Patient Data;
- Use Patient Data for advertising or marketing;
- Use Patient Data to train artificial intelligence or machine learning models without the explicit written instruction of the Data Fiduciary and any patient consent required by law.

9.5 Security. KramOS implements reasonable technical and organisational measures to protect Patient Data, as described in clause 14.

9.6 Cross-border transfer. Patient Data is stored on data centres located in India unless the Institution explicitly instructs otherwise. KramOS will not transfer Patient Data outside India contrary to applicable Indian law.

9.7 Sub-processors. Where KramOS engages sub-processors (such as cloud hosting providers), it does so under contractual obligations consistent with this Policy.

9.8 Return and deletion. Upon termination of the Institution's contract, KramOS will, for a reasonable period (typically thirty (30) days), allow the Institution to export Patient Data. Thereafter, KramOS will delete Patient Data in accordance with the retention practices in clause 13, unless retention is required by law.

10. ABDM AND HEALTHCARE INTEROPERABILITY

The Services are designed to be compatible with the architecture of the Ayushman Bharat Digital Mission ("ABDM"). Where you or your Institution choose to enable ABDM-linked features (such as Health ID linking or consent-based health record exchange), additional notices and consents under the ABDM framework will apply.

KramOS does not link to ABDM or share health records via ABDM without explicit consent from the Institution and the patient where required.

11. COOKIES AND SIMILAR TECHNOLOGIES

11.1 The Site uses cookies and similar technologies to:

- Operate the Site (essential cookies — strictly necessary for login, security, and session management);
- Remember your preferences (functional cookies);
- Understand how the Site is used and improve it (analytics cookies);
- Measure marketing campaigns (advertising and tracking cookies — only with consent).

11.2 You can control cookies through your browser settings and through the cookie banner on the Site. Disabling essential cookies may affect Site functionality.

11.3 We use the following types of analytics tools: web analytics (e.g. Google Analytics or similar), product analytics for in-product behaviour, and basic server-side logging. Where these tools collect Personal Data, we apply IP anonymisation where supported and limit retention to the minimum necessary.

12. WHO WE SHARE PERSONAL DATA WITH

We share Personal Data only with the following categories of recipients, and only to the extent necessary:

12.1 **Service providers and sub-processors** — including cloud hosting providers, payment gateways, email and WhatsApp messaging providers, analytics providers, customer support platforms, and software development tools. These providers are contractually obliged to protect Personal Data and use it only for the purposes we specify.

12.2 **The Institution and its authorised users** — within the relevant Institution, Personal Data of users and patients is accessible only to those users authorised under the Institution's own role-based access controls.

12.3 **Professional advisors** — including auditors, accountants, lawyers, and consultants, under appropriate confidentiality obligations.

12.4 **Authorities and law enforcement** — where required by law, court order, or in response to a lawful request, including under the IT Act, the DPDP Act, and the Code of Criminal Procedure, 1973.

12.5 **Corporate transactions** — in the context of a merger, acquisition, financing, or reorganisation, subject to appropriate confidentiality and data protection commitments.

12.6 **With your consent** — where you have specifically asked us to share data with a third party.

We do **not** sell Personal Data to anyone. We do not share Patient Data for marketing, advertising, or profiling.

13. DATA RETENTION

13.1 We retain Personal Data only for as long as necessary to fulfil the purposes set out in this Policy or as required by law.

13.2 Approximate retention periods:

- **Waitlist signups:** Until you ask to be removed or until the relevant product has launched and you have either subscribed or declined to subscribe, whichever is earlier.
- **Account data:** For the duration of your Account, and for up to three (3) years after termination, unless a longer period is required by law (for example, tax records under the Income Tax Act, 1961).
- **Billing and tax records:** As required under applicable tax and accounting laws, typically eight (8) years.
- **Patient Data:** Retained as long as the Institution's contract requires, and deleted in accordance with clause 9.8 after termination, unless the Institution or applicable law requires longer retention.
- **Server logs and security records:** Typically 90 to 180 days, longer if necessary for security investigation.
- **Marketing data:** Until you opt out, or for two (2) years of inactivity, whichever is earlier.

13.3 When Personal Data is no longer needed, it is deleted, anonymised, or aggregated in a manner that prevents re-identification.

14. DATA SECURITY

KramOS implements reasonable technical and organisational security measures to protect Personal Data and Patient Data, including:

- **Encryption** in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent);
- **Access controls** — role-based access, principle of least privilege, multi-factor authentication for administrative access;
- **Audit logs** — comprehensive logs of access to and modification of Personal Data and Patient Data;
- **Network and infrastructure security** — firewalls, intrusion detection, regular security scanning;
- **Sub-processor due diligence** — vetting and contracting with cloud providers and other sub-processors;
- **Personnel safeguards** — confidentiality agreements, security training, background checks for sensitive roles;
- **Incident response** — a documented process for detecting, investigating, and responding to security incidents;
- **Backups** — encrypted, periodic backups with controlled restoration procedures.

No system is completely secure, and we cannot guarantee absolute security. We will notify affected users and the Data Protection Board of India of a personal data breach in the manner and within the timelines required by the DPDP Act.

15. YOUR RIGHTS AS A DATA PRINCIPAL

Subject to the DPDP Act and other applicable law, you have the following rights in respect of your Personal Data:

15.1 **Right to access** — to obtain a summary of the Personal Data we process about you and the processing activities we have undertaken.

15.2 **Right to correction and erasure** — to have inaccurate or misleading Personal Data corrected, completed, updated, or erased.

15.3 **Right to grievance redressal** — to raise a grievance with our Grievance Officer (clause 19).

15.4 **Right to nominate** — to nominate another individual to exercise your rights in the event of your death or incapacity.

15.5 **Right to withdraw consent** — where processing is based on consent, you may withdraw it at any time. Withdrawal does not affect the lawfulness of processing before withdrawal.

To exercise any of these rights, please write to privacy@kramos.health from the email address on your Account, or contact the Grievance Officer. We will respond within the timelines prescribed under the DPDP Act.

For Patient Data, requests should be directed to the Institution that is the Data Fiduciary. KramOS will assist the Institution in responding to such requests in its capacity as Data Processor.

16. CHILDREN'S DATA

The Services are not directed at, intended for, or marketed to individuals under the age of 18. We do not knowingly collect Personal Data of minors as direct users.

In a clinical setting, the Services may process Patient Data of paediatric patients. Such processing is undertaken solely on the instructions of the Institution, which is responsible for ensuring that any consents required from a parent or guardian have been obtained in accordance with applicable law.

If we become aware that we have inadvertently collected Personal Data of a minor as a direct user, we will delete it.

17. THIRD-PARTY LINKS

The Site and Services may contain links to third-party websites or services (for example, payment gateways, ABDM, or training resources). KramOS is not responsible for the privacy practices of third parties. We encourage you to review the privacy policies of any third-party site before providing your Personal Data.

18. MARKETING COMMUNICATIONS AND WHATSAPP

18.1 With your consent, we may send marketing communications about KramOS products, features, and content by email, WhatsApp, SMS, or telephone.

18.2 You may opt out of marketing communications at any time by:

- Clicking the "unsubscribe" link in any marketing email;
- Replying "STOP" to a WhatsApp or SMS message;
- Writing to privacy@kramos.health.

18.3 Opting out of marketing does not affect Service-related communications (such as billing notices, security alerts, and important Service updates), which are necessary for the operation of your Account.

18.4 WhatsApp communications are sent through a registered Business Solution Provider in compliance with the WhatsApp Business Policy and Indian telecom regulations.

19. GRIEVANCE OFFICER AND DATA PROTECTION CONTACT

In accordance with the IT Act, the SPDI Rules, and the DPDP Act, we have appointed a Grievance Officer to address concerns regarding Personal Data and the operation of the Services.

Grievance Officer

Name: [NAME]

Email: grievance@kramos.health

Address: Kaizen Health Technologies Private Limited, [REGISTERED ADDRESS], Bengaluru, Karnataka, India

We will acknowledge grievances within seventy-two (72) hours and aim to resolve them within fifteen (15) days, or such shorter timeline as is required by applicable law.

If your grievance is not resolved to your satisfaction, you have the right to escalate the matter to the Data Protection Board of India, once constituted, in accordance with the DPDP Act.

20. INTERNATIONAL TRANSFERS

KramOS is an India-based company, and our default position is that Personal Data and Patient Data are processed within India.

We may transfer Personal Data outside India only where:

- Permitted under the DPDP Act and applicable rules;
- Subject to contractual safeguards equivalent to those applicable in India;
- Notified to and accepted by you (or, in the case of Patient Data, the relevant Institution).

We will not transfer Patient Data to any jurisdiction that the Government of India has notified as restricted.

21. CHANGES TO THIS PRIVACY POLICY

21.1 We may revise this Privacy Policy from time to time. The most current version will be posted at <https://kramos.health/privacy> with a revised "Last Updated" date.

21.2 Where a revision materially changes how we process Personal Data, we will notify you by email or through the Services at least fifteen (15) days before the change takes effect.

21.3 Continued use of the Services after the effective date of a revised Policy constitutes acceptance of those changes.

22. CONTACT US

For any privacy-related questions, requests, or concerns:

Kaizen Health Technologies Private Limited

[REGISTERED ADDRESS]

Bengaluru, Karnataka, India

Privacy: privacy@kramos.health

Grievance Officer: grievance@kramos.health

Security incidents: security@kramos.health

General: hello@kramos.health

Privacy is not a feature we added to KramOS. It is the floor we built it on.